# Appendix F

# Use of City Equipment and Social Media Policy

## Cell Phones and other devices

This policy applies to employee use of cell phones, smart phones (including iPhones, Androids, and similar devices), tablets and similar devices, all of which are referred to as "Cellular Devices".

Cell Phones and Cellular Devices in General (both City provided and personal cell phones/cellular devices)

Employees are allowed to bring personal cell phones and Cellular Devices to work with them. During working hours, however, employees should refrain from using them except in an emergency or during a meal period or rest break.

Employees who use personal or City provided cell phones/Cellular Devices may not violate City's policies against harassment and discrimination. Thus, employees who use a personal or City - provided cell phone/Cellular Device to send a text or instant message to another employee (or to a citizen or someone not employed by the City ) that is harassing or otherwise in violation of City's no-harassment and no-discrimination policies will be subject to discipline up to and including termination.

Non-exempt employees may not use their personal or City provided cell phone/Cellular Device for work purposes outside of their normal work schedule without authorization in advance from supervisor. This includes, but is not limited to, reviewing, sending and responding to emails or text messages, and responding to calls or making calls. Employees who violate this policy may be subject to discipline, up to and including termination.

## Employee Use of City Provided Cell Phones/Cellular Devices

Cell phones/Cellular Devices are made available to City employees on a limited basis to conduct City's business. Determinations as to which employees receive City provided cell phones will be made on a case-by-case basis; employees are not guaranteed a cell phone or cellular device.

Employees who receive a cell phone or cellular device from City must agree to only use the cell phone/Cellular Device for minimal personal use. Further, employees who receive a cell phone or cellular device from the City must acknowledge and understand that because the cell phone/cellular device is paid for and provided by the City, any communications (including text messages) received by or sent from the cell phone/cellular device may be subject to inspection and review if the City has reasonable grounds to believe that the employee's use of the cell phone violates any aspect of the City policy. An employee who refuses to provide the City access

to his/her personal cell phone/cellular device in connection with an investigation and after reasonable notice may be subject to discipline, up to and including termination.

Employees may not use the City provided cell phones or cellular devices to call 1-900, 1-976 or similar "pay per minute" services. Further, family and friends may not use an employee's City provided cell phone/cellular device.

## Cell Phones/Cellular Devices and Public Records

City related business conducted on City provided or personal cell phones/cellular devices, may be subject to disclosure under Oregon's Public Records laws.

## Cell Phone/Cellular Device Use While Driving

The use of a cell phone or cellular device while driving may present a hazard to the driver, other employees and the general public. Subject to a few narrow exceptions for emergency or public safety purposes, Oregon law also prohibits the use of hand-held cell phones while driving, even if the driving is for work-related reasons. This policy is meant to ensure the safe operation of City vehicles and the operation of private vehicles while an employee is on work time. It applies equally to the usage of employee-owned cell phones and phones provided or subsidized by City.

Employees are prohibited from using hand-held cell phones for any purpose while driving on City authorized or City related business. This policy also prohibits employees from using a cell phone or other device to send or receive text or "instant" messages while driving on City business. Should an employee need to make a business call while driving, the employee must locate a lawfully designated area to park and make the call, unless the employee uses a hands-free cell phone or cellular device for the call. In either situation, such calls should be kept short and should the circumstances warrant (for example, heavy traffic, bad weather), the employee should locate a lawfully designated area to park to continue or make the call, even if the employee is using a hands-free device. Violation of this policy will subject the employee to discipline, up to and including termination.

## Use of City Email and Electronic Equipment, Facilities and Services

The City of Newberg uses multiple types of electronic equipment, facilities and services for producing documents, research and communication including, but not limited to, computers, software, e-mail, copiers, telephones, voicemail, fax machines, online services, cell phones (including text messaging), the Internet and any new technologies used in the future. This policy governs the use of such City property.

## Ownership

All information and communications in any format, stored by any means on or received via City's electronic equipment, facilities or services is the sole property of the City of Newberg.

## Use

All of City's electronic equipment, facilities and services are provided and intended for City business purposes, may be used for occasional personal matters or communications. All access by employee may be subject to public records request and reviewed by the City, employees may not use the City provided Internet, or City electronic equipment, facilities and services to:

- Display or store any sexually explicit images or documents, or any images or documents that would violate City's no-harassment, no-discrimination or bullying policies;
- Engage in any activity that violates the rights of any person or company protected by copyright, trade secrets, patent or other intellectual property (or similar laws or regulations);
- Engage in any activity that violates the rights to privacy of protected healthcare information or other City specific confidential information;
- Engage in any activity that would introduce malicious software purposefully into a workstation or network (e.g., viruses, worms, Trojan horses).
- Download or view streaming video for personal use. This includes, without limitation, YouTube videos, and movies and TV shows. Streaming audio is allowed, providing it does not contain explicit material, adversely affect network speed, or interfere with others' ability to work.

Further, employees may not use City provided email addresses to create or manage personal accounts (e.g., shopping websites, personal bank accounts, and social media accounts). City email addresses for professional-based social media accounts such as LinkedIn may be allowed with the approval of the employee's supervisor.

## Inspection and Monitoring

Employee communications, both business and personal, made using City electronic equipment, facilities, and services are not private. Any data created, received or transmitted using City equipment, facilities or services are the property of City and usually can be recovered even though deleted by the user.

All information and communications in any format, stored by any means on City's electronic equipment, facilities or services, are subject to inspection at any time without notice. Personal passwords may be used for purposes of security, but the use of a personal password does not affect City's ownership of the electronic information, electronic equipment, facilities, or services, or City's right to inspect such information. The City reserves the right to access and review electronic files, documents, archived material, messages, email, voicemail and other such material to monitor the use of all of City's electronic equipment, facilities and services,

including all communications and internet usage and resources visited. The City will override all personal passwords if it becomes necessary to do so for any reason.

## Personal Hardware and Software

Employees may not install personal hardware or software on City's computer systems without approval from the City. All software installed on the City's computer systems must be licensed. Copying or transferring of City owned software may be done only with the written authorization of the employees' director supervisor.

## Unauthorized Access

Employees are not permitted unauthorized access to the electronic communications of other employees or third parties unless directed to do so by the City Manager. No employee can examine, change or use another person's files, output or user name unless they have explicit authorization to do so.

## Security

Many forms of electronic communication are not secure. Employees who use cell phones, cordless phones, fax communications or email sent over the Internet should be aware that such forms of communication are subject to interception and these methods of communicating should not be used for privileged, confidential, or sensitive information unless appropriate encryption measures are implemented.

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

All personal computers, laptops, and workstations should be secured with password protected screen savers with an automatic activation feature, set at ten minutes or less, or by logging off (control-alt-delete) when the computer is unattended.

## Inappropriate Web Sites

City's electronic equipment, facilities or services must not be used to visit Internet sites that contain obscene, hateful or other objectionable materials, or that would otherwise violate City's policies on harassment and discrimination.

## Social Media

For purposes of this policy, "social media" includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, commercial web site, social networking web site or app, web bulletin board or a chat room, whether or not associated or affiliated with the City, as well as any other form of electronic communication.

Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of co-workers, or otherwise adversely affects our citizens or people who work on behalf of the City or City's legitimate business interests, may result in disciplinary action up to and including termination.

## Prohibited Postings

Employees will be subject to discipline, up to and including termination, if they create and post any text, images or other media that violate the City's no-harassment and no-discrimination policies, or that include threats of violence or similar inappropriate or unlawful conduct.

Do not create a link from your blog, website or other social networking site to a City owned or maintained website without identifying yourself as an City employee.

Never represent yourself as a spokesperson for the City. Express only your personal opinions. If the City is a subject of the content you are creating, be clear and open about the fact that you are a City employee, and make it clear that your views do not represent those of the City or its employees or elected officials.

## Encouraged Conduct

Always be fair and courteous to co-workers, the citizens we serve, City employees and elected officials, and suppliers or other third parties who do business with the City. Also, keep in mind that you are more likely to resolve work-related complaints by speaking directly with your co-workers or by utilizing our Open Door Policy than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage citizens, co-workers, City employees or elected officials, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or City policy.

Maintain the confidentiality of the City's information. Do not post internal reports, personnel records, information or documents designated as "confidential" by law or City policy, or other internal, City-related confidential communications or information. See "Confidential City Information," below.

Nothing in this policy is meant to prevent an employee from exercising his or her right to make a complaint of discrimination or other workplace misconduct, engage in lawful collective bargaining activity, or to express an opinion on a matter of public concern that does not unduly disrupt the City's operations.

## Request for Employee Social Media Passwords

City supervisors and department directors are prohibited by law from requiring or requesting an employee or an applicant for employment to disclose or to provide access through the employee's or applicant's user name and password, password or other means of authentication that provides access to a personal social media account. This includes, without limitation, a user name and password that would otherwise allow a supervisor/department director to access a private email account not provided by the City, or a demand to "friend" someone on Facebook.

Nothing in this policy prohibits the City from requiring an employee to produce content from his or her social media or internet account in connection with a City sponsored investigation into potential misconduct, unlawful or unethical behavior, or policy or rule violations.

## Confidential City Information

Employees must not access, use or disclose sensitive or confidential information or data except in accordance with City policies, practices and procedures, and as authorized by state or federal laws or regulations. Employees with access to confidential information, including but not limited to customer or employee financial, medical or personal information (including, without limitation, Social Security numbers), are responsible for the safekeeping and handling of that information to prevent unauthorized disclosure. Employees who access, use or disclose confidential information contrary to Oregon or federal laws or for personal use or financial gain may be subject to civil or criminal penalties under those laws, in addition to appropriate disciplinary action for violating this policy.

No records or information including (without limitation) protected medical data, documents, files, records, computer files or similar materials (except in the ordinary course of performing duties on behalf of the City may be removed from our premises without permission from the supervisor. Likewise, any materials developed by City's employees in the performance of their jobs is the property of City and may not be used for personal or financial gain. Additionally, the contents of records or information otherwise obtained in regard to the City's business may not be disclosed to anyone, except where required for a business purpose or when required by law.

## Misuse Notification

Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, the City of Newberg will establish an operational incident handling capability for all information systems with access to FBI CJIS systems and data. This includes adequate preparation, detection, analysis, containment, recovery, and user response activities; track, document, and report incidents to appropriate agency officials and/or authorities.